Application of Standards to Accelerator Safety Systems

Sandra L. Prior, REM, CHMM

System Safety and Safety Systems for Accelerators

US Particle Accelerator School

June 28 – July 2, 2004

Why Do I Have to Have a Safety System?

- Legal requirements
- Good Business practices
- Liability reduction
- Competition for resources
- Mission accomplishment

Aren't Administrative Controls Good Enough?

- Not as effective as engineering controls
- Criticized as means of spreading exposures rather than eliminating or reducing them
- Depend upon continual human intervention
- Difficult to implement and maintain
- May be more expensive over the long term

What Are The Hazards Associated With Accelerators?

- Prompt Ionizing Radiation
- Residual Ionizing Radiation
- Oxygen Deficiency
- Fire/Explosive (Hazardous Classified) Areas
- Laser Radiation
- Other Non-Ionizing EM Radiation
- Open Machinery
- Exposed Electrical Equipment
- Chemical Processes
- Biological Research Facilities

Who Has Legal Authority Over Accelerators?

- OSHA covers all radiation sources not regulated by A.E.C.
  - Examples of non-A.E.C. regulated radiation sources include X-ray equipment, accelerators, accelerator-produced materials, electron microscopes, betatrons, and some naturally occurring radioactive materials.

Accelerator System Design and Implementation

- Very little specific requirements on accelerators exist in law/regulations
  - 10 CFR 835
  - 29 CFR 1910.1096
  - 29 CFR 1910, Subpart S
- OSHA's Process Safety Standard, 29 CFR 1910.119, contains some guidance but is not applicable to accelerators
- Must defer to consensus standards for guidance

OSHA General Duty Clause (GDC)

Section 5 of the OSH Act or the "General Duty Clause" which states:

A. Each Employer:

1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or likely to cause death or serious physical harm to his employees;

2) shall comply with occupational safety and health standards promulgated under this Act.

OSHA General Duty Clause (GDC)

Section 5 of the OSH Act or the "General Duty Clause" which states:

B. Each employee shall comply with occupational safety and health standards and all rules, regulations and orders issued pursuant to this Act which are applicable to his own actions and conduct.

OSHA GDC Criteria

- The employer failed to keep the work place free of a hazard to which employees of that employer were exposed.
- The hazard is (or should have been) recognized by the employer.
- The hazard is causing or was likely to cause death or other serious physical harm.
- There is a feasible and useful method to correct the hazard.

Why Consensus Standards?

- Establish a context where ideas and solutions can be exchanged
- Focused on quality outcomes
- Part of an overall risk management plan
- Provide you a sound basis for your documented justification

Types of Standards

- Implementation Prescriptive
  - Nuclear Industry
  - Air Craft
  - Space
- Consensus
  - Process Industries
  - Manufacturing Industries
  - Research and Development

Public Law 104-113

National Technology Transfer and
Advancement Act of 1995 [Public Law (PL) 104-113]

"Federal Participation in the Development and Use of Voluntary Standards…"

"PL 104-113 is a true shift in the paradigm for many Federal agencies regarding the conduct of their technical standards activities. Where DOE, in its continued transition to a "work smart", standards-based operating culture, identifies the need for new or revised technical standards, PL 104-113 compels us to focus all technical standards development efforts deemed necessary toward voluntary standards in lieu of DOE technical standards. "

Assistant Secretary for EH

Consensus Standards

- Both National and International
- Voluntary
- May become regulatory when:
  - Referenced in law/regulation
  - Incorporated into agreements
  - May reference entire document or only portions
- May become an implied requirement

How Do I Determine What Consensus Standards To Follow?

- Identify standards that are applicable to a wide group of users.
- Identify standards that add value to the organization and tasks at hand.
- Identify standards that are not obsolete the day they are published.
- The trick then is to translate these standards into commitments that are not overly prescriptive.

Possible Accelerator Safety System Standards

ANSI/ISA S84, Application of Safety Instrumented Systems for the Process Industries

IEC 61508-1, Functional safety of electrical/ electronic/programmable electronic safety-related systems

IEC 61511, Functional safety – Safety instrumented systems for the process industry sector

MIL-STD-882D, Standard Practice for System Safety

IEC 62198, Project Risk Management

IEC 61131-3, Programming Industrial Automation Systems

Possible Accelerator Safety System Standards (continued)

IEC 1025, Fault Tree Analysis NCRP 88, Radiation Alarms and Access Control Systems

ISO 9001:2000, Quality Management Systems

ISO 14001, Environmental Management Systems

ISO 18001, Occupational Health & Safety Management Systems

ANSI/ISA S84.01

- Consensus Standard
- Designed to meet Needs of Process Industry, e.g. 10CFR1910.119
- Wide Body of Experience
  - Equipment Manufacturers
  - System Integrators
  - Reliability Engineers
  - Academia
- Deals mostly with the programmable section of the safety system

S84 Key Points

- Requires Hazard Identification and Classification
- Safety Requirements Specification
  - Identify Safety Functions
  - Identify Required SIL for Safety Systems
  - Identify Safe State
- Safety Implementation
- Evaluation of Proposed Design
- Management of Change Plan

S84 and OSHA

March 31, 2000 - "As S84.01 is a national consensus standard, OSHA considers it to be a recognized and generally accepted good engineering practice for SIS (Safety Instrumented Systems),"

Richard E. Fairfax, Director, Directorate of Compliance Program Assistance for OSHA

Refers to S84 in the context of requirements of 10CFR1910.119 Hazardous Chemical Controls

ISA-TR84.02

- Guidance to S84 for determining safety integrity level (SIL) of a safety system
- Gives Three methods for calculating SIL
  - Simplified Equations (Block Diagram)
  - Fault Tree
  - Markov Model
- Part 5 gives methods for calculation of PFD of logic solver using Markov models.

IEC61508

- Umbrella Standard intended to cover all industrial safety system applications –E/E/PE
- Meant as starting point for sector standards
- Very detailed, almost prescriptive
- Defines key numerical risk reduction criteria
- Intended for manufacturers

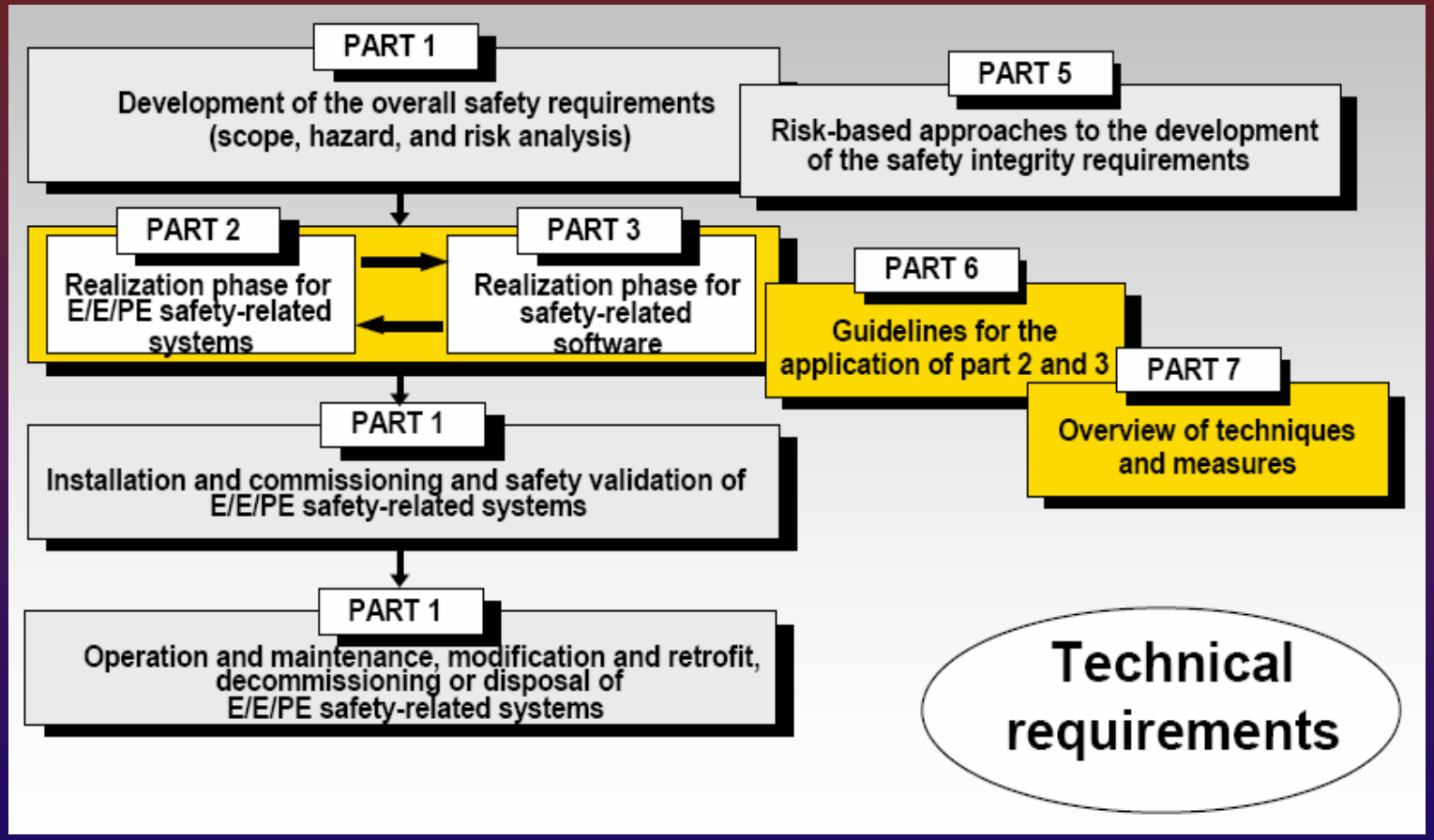
IEC61508

- 7 Parts
  - Part 1 General Requirements
  - Part 2 Systems Requirements
  - Part 3 Software Requirements
  - Part 4 Definitions
  - Part 5 SIL Evaluation methods
  - Part 6 Guidelines on applying parts 1 and 2
  - Part 7 Overview of techniques

Normative

Informative

IEC 61508 – Functions of Parts 1-7



Exida's *Introduction to IEC 61508,* http://www.exida.com/training/

‘In Country’ Clause

IEC61508 Part 1.4…

“In the USA and Canada, until the proposed sector implementation of IEC 61508 is published as an international standard in the USA and Canada, existing national process safety standards based on IEC61508 (i.e. ANSI/ISA S84.01-1996) can be applied to the process sector instead of IEC61508.”

IEC61511

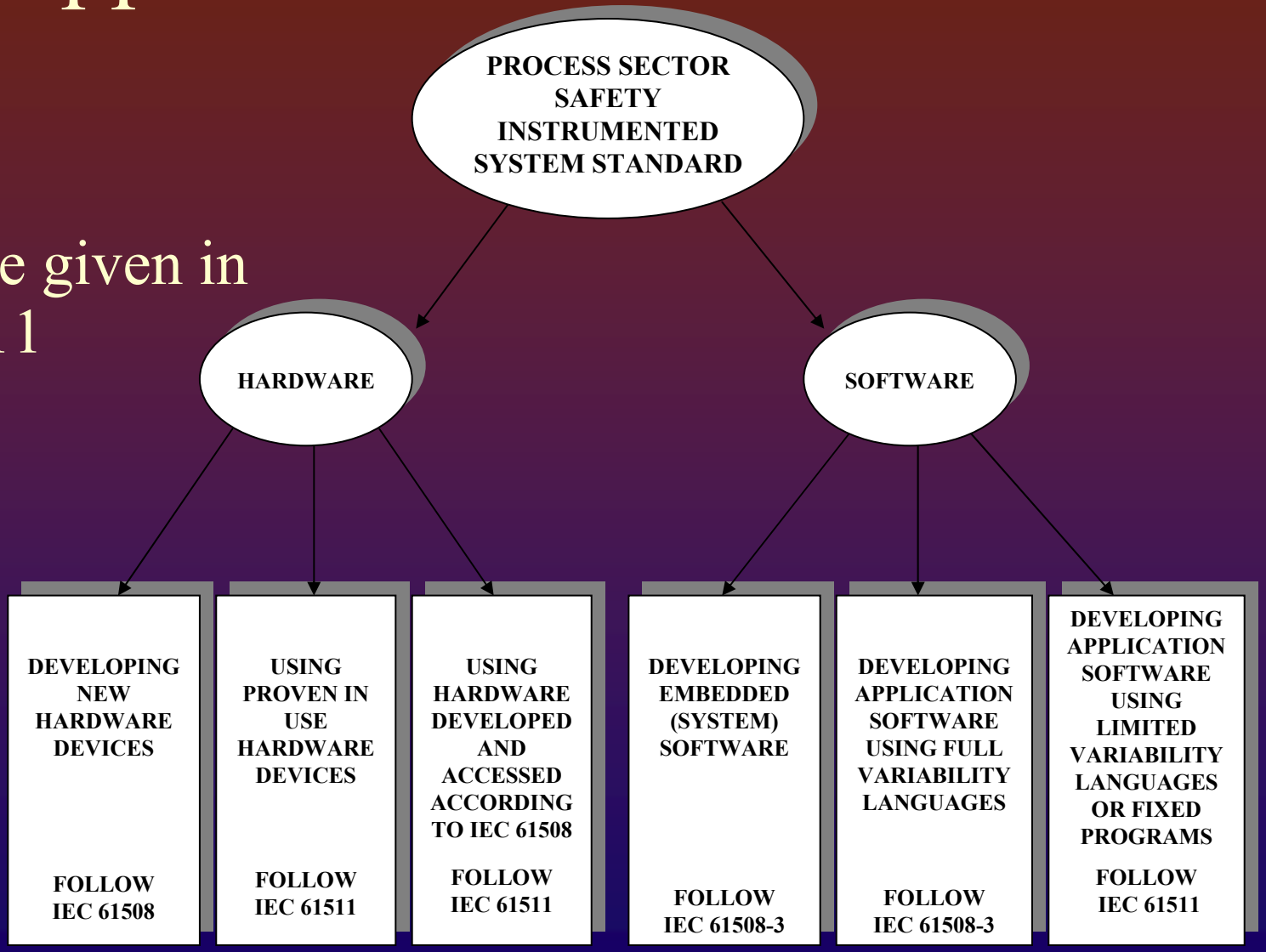
- IEC revision of process sector standards, e.g. ANSI/ISAS84.01
- Released in February 2003
- 3 Parts
  - Part 1 General Requirements
  - Part 2 Guidelines for application
  - Part 3 Guidelines for Hazard and Risk Analysis

Software

- Languages
  - IEC61131-3 Defines PLC programming Languages
- Applications
  - Software application development is left to “Good Practice”
  - A good start is in IEC 61508 and 61511
  - IEC880 (Software for Computers in the Safety Systems of Nuclear Power Stations) is a good reference

Application of IEC Standards

Guidance given in IEC61511



Basis for OSHA/NRC Evaluation

- Safety program conforms to accepted “good practice”
- Personnel are recognized as “competent” in their field
- Safety programs are well documented
  - Hazard/Risk Analyses
  - Design & design basis
  - Testing/Certification
  - Procedures
  - Training
  - Corrective Action

What is Your Legal Basis?

California
New Mexico
New York
Brazil
Illinois
Tennessee
Utah
DOE